Host Identity Protocol (HIP) Domain Name System (DNS) Extensions
draft-ietf-hip-dns-07

Status of this Memo

   By submitting this Internet-Draft, each author represents that any
   applicable patent or other IPR claims of which he or she is aware
   have been or will be disclosed, and any of which he or she becomes
   aware will be disclosed, in accordance with Section 6 of BCP 79.

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF), its areas, and its working groups. Note that
   other groups may also distribute working documents as Internet-
   Drafts.

   Internet-Drafts are draft documents valid for a maximum of six months
   and may be updated, replaced, or obsoleted by other documents at any
   time. It is inappropriate to use Internet-Drafts as reference
   material or to cite them other than as "work in progress."

   The list of current Internet-Drafts can be accessed at
   http://www.ietf.org/ietf/1id-abstracts.txt.

   The list of Internet-Draft Shadow Directories can be accessed at
   http://www.ietf.org/shadow.html.

   This Internet-Draft will expire on March 31, 2007.

Copyright Notice

Abstract

   This document specifies a new resource record (RR) for the Domain
   Name System (DNS), and how to use it with the Host Identity Protocol
   (HIP.) This RR allows a HIP node to store in the DNS its Host
   Identity (HI, the public component of the node public-private key
   pair), Host Identity Tag (HIT, a truncated hash of its public key),
   and the Domain Names of its rendezvous servers (RVS.)

Table of Contents

[1](#). **Introduction**

   This document specifies a new resource record (RR) for the Domain
   Name System (DNS) [RFC1034], and how to use it with the Host Identity
   Protocol (HIP) [I-D.ietf-hip-base]. This RR allows a HIP node to
   store in the DNS its Host Identity (HI, the public component of the
   node public-private key pair), Host Identity Tag (HIT, a truncated
   hash of its HI), and the Domain Names of its rendezvous servers
   (RVS.) [I-D.ietf-hip-rvs]

   Currently, most of the Internet applications that need to communicate
   with a remote host first translate a domain name (often obtained via
   user input) into one or more IP address(es). This step occurs prior
   to communication with the remote host, and relies on a DNS lookup.

   With HIP, IP addresses are intended to be used mostly for on-the-wire
   communication between end hosts, while most ULPs and applications use
   HIs or HITs instead (ICMP might be an example of an ULP not using
   them.) Consequently, we need a means to translate a domain name into
   an HI. Using the DNS for this translation is pretty straightforward:
   We define a new HIP resource record. Upon query by an application or
   ULP for a FQDN -> IP lookup, the resolver would then additionally
   perform an FQDN -> HI lookup, and use it to construct the resulting
   HI -> IP mapping (which is internal to the HIP layer.) The HIP layer
   uses the HI -> IP mapping to translate HIs and HITs into IP addresses
   and vice versa.

   The HIP rendezvous extensions [I-D.ietf-hip-rvs] proposal allows a
   HIP node to be reached via the IP address(es) of a third party, the
   node's rendezvous server (RVS.) An initiator willing to establish a
   HIP association with a responder served by a RVS would typically
   initiate a HIP exchange by sending an I1 towards the RVS IP address
   rather than towards the responder IP address. Consequently, we need
   a means to translate a domain name into the rendezvous server's
   domain name.

   This draft introduces the new HIP DNS Resource Record to store
   Rendezvous Server (RVS), Host Identity (HI) and Host Identity Tag
   (HIT) information.

2. Conventions used in this document

   The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
   "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
   document are to be interpreted as described in RFC2119 [RFC2119].

3. Usage Scenarios

   In this section, we briefly introduce a number of usage scenarios
   where the DNS is useful with the Host Identity Protocol.

   With HIP, most application and ULPs are unaware of the IP addresses
   used to carry packets on the wire. Consequently, a HIP node could
   take advantage of having multiple IP addresses for fail-over,
   redundancy, mobility, or renumbering, in a manner which is
   transparent to most ULPs and applications (because they are bound to
   HIs, hence they are agnostic to these IP address changes.)

   In these situations, a node wishing to be reachable by reference to
   its FQDN should store the following information in the DNS:

   o A set of IP address(es) through A and AAAA RRs.

   o A Host Identity (HI), Host Identity Tag (HIT) and possibly a set
      of rendezvous server(s) (RVS) through HIP RRs.

   When a HIP node wants to initiate a communication with another HIP
   node, it first needs to perform a HIP base exchange to set-up a HIP
   association towards its peer. Although such an exchange can be
   initiated opportunistically, i.e., without prior knowledge of the
   responder's HI, by doing so both nodes knowingly risk man-in-the-
   middle attacks on the HIP exchange. To prevent these attacks, it is
   recommended that the initiator first obtain the HI of the responder,
   and then initiate the exchange. This can be done, for example,
   through manual configuration or DNS lookups. Hence, a new HIP RR is
   introduced.

   When a HIP node is frequently changing its IP address(es), the
   dynamic DNS update latency may prevent it from publishing its new IP
   address(es) in the DNS. For solving this problem, the HIP
   architecture introduces rendezvous servers (RVS.) A HIP host uses a
   rendezvous server as a rendezvous point, to maintain reachability
   with possible HIP initiators. Such a HIP node would publish in the
   DNS its RVS domain name(s) in a HIP RR, while keeping its RVS up-to-
   date with its current set of IP addresses.

   When a HIP node wants to initiate a HIP exchange with a responder it
   will perform a number of DNS lookups. Depending on the type of the
   implementation, the order in which those lookups will be issued may
   vary. For instance, implementations using HIT in APIS may typically
   first query for HIP resource records at the responder FQDN, while
   those using IP address in APIs may typically first query for A and/or
   AAAA resource records.

In the following we assume that the initiator first queries for HIP
resource records at the responder FQDN.

If the query for the HIP type was responded to with a DNS answer with
RCODE=3 (Name Error), then the responder's information is not present
in the DNS and further queries SHOULD NOT be made.

In case the query for the HIP records returned a DNS answer with
RCODE=0 (No Error), then the initiator sends out one more query for
for A and AAAA types at the responder's FQDN.

Depending on the combinations of answer the situations described in
Section 3.1 and Section 3.2 can occur.

Note that storing HIP RR information in the DNS at a FQDN which is
assigned to a non-HIP node might have ill effects on its reachability
by HIP nodes.

3.1. Simple static singly homed end-host

A HIP node (R) with a single static network attachment, wishing to be
reachable by reference to its FQDN (www.example.com), would store in
the DNS, in addition to its IP address(es) (IP-R), its Host Identity
(HI-R) and Host Identity Tag (HIT-R) in a HIP resource record.

An initiator willing to associate with a node would typically issue
the following queries:

    QNAME=www.example.com, QTYPE=HIP

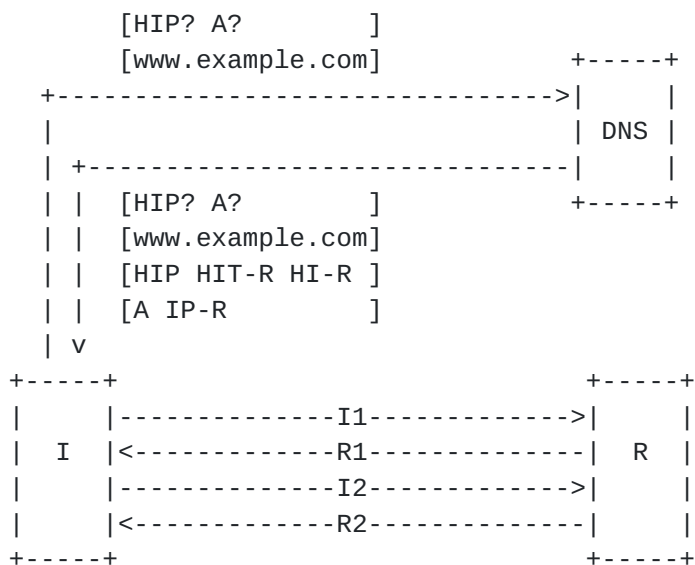   (QCLASS=IN is assumed and omitted from the examples)

Which returns a DNS packet with RCODE=0 and one or more HIP RRs with
the HIT and HI (e.g. HIT-R and HI-R) of the responder in the answer
section, but no RVS.

    QNAME=www.example.com, QTYPE=A

Which returns a DNS packet with RCODE=0 and one or more A or AAAA RRs
containing IP address(es) of the responder (e.g. IP-R) in the answer
section.

Caption: In the remainder of this document, for the sake of keeping
         diagrams simple and concise, several DNS queries and answers
         are represented as one single transaction, while in fact
         there are several queries and answers flowing back and
         forth, as described in the textual examples.

          [HIP? A?   ]
          [www.example.com]   +-----+
       +--------------------------------->| |
       | | DNS |
       | +------------------------------| |
       | | [HIP? A?   ]   +-----+
       | | [www.example.com]
       | | [HIP HIT-R HI-R]
       | | [A IP-R   ]
       | v
     +-----+   +-----+
     | |--------------I1------------->| |
     | I |<-------------R1--------------| R |
     | |--------------I2------------->| |
     | |<------------R2--------------| |
     +-----+   +-----+

   The initiator would then send an I1 to the responder's IP addresses
   (IP-R.)

3.2. Mobile end-host

   A mobile HIP node (R) wishing to be reachable by reference to its
   FQDN (www.example.com) would store in the DNS, possibly in addition
   to its IP address(es) (IP-R), its HI (HI-R), HIT (HIT-R) and the
   domain name(s) of its rendezvous server(s) (rvs.example.com) in HIP
   resource record(s). The mobile HIP node also needs to notify its
   rendezvous servers of any change in its set of IP address(es).

   An initiator willing to associate with such mobile node would
   typically issue the following queries:
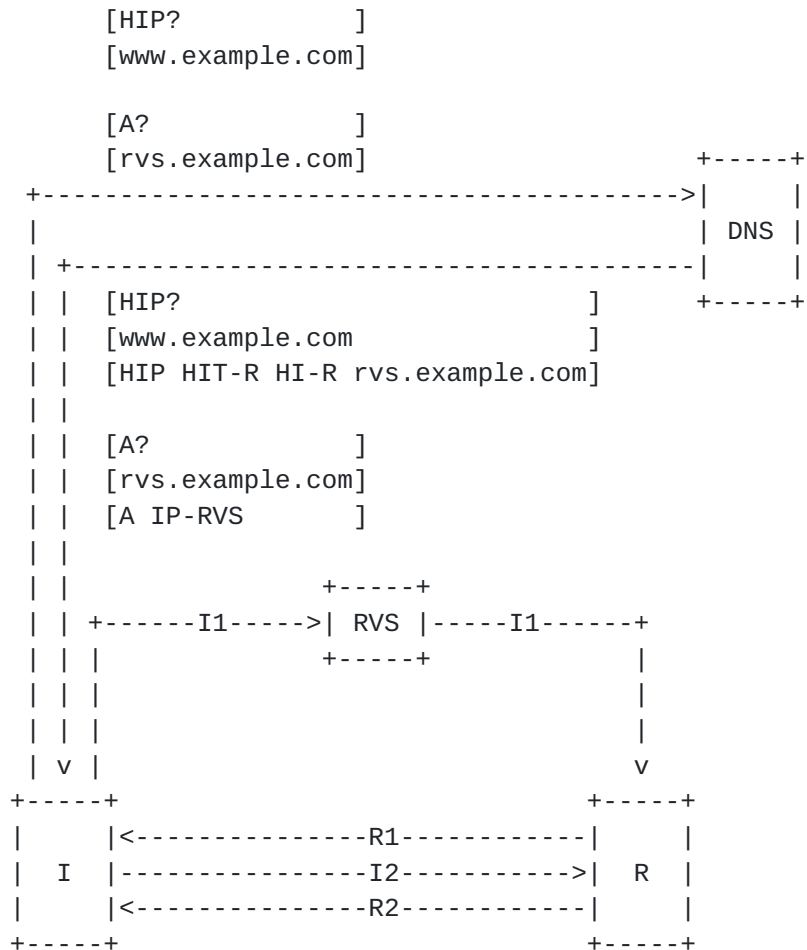
      QNAME=www.example.com, QTYPE=HIP

   Which returns a DNS packet with RCODE=0 and one or more HIP RRs with
   the HIT, HI and RVS domain name(s) (e.g. HIT-R, HI-R, and
   rvs.example.com) of the responder in the answer section.

      QNAME=rvs.example.com, QTYPE=A

   Which returns a DNS packet with RCODE=0 and one or more A or AAAA RRs

containing IP address(es) of the responder's RVS (e.g. IP-RVS) in
the answer section.

```
          [HIP?            ]
          [www.example.com]

          [A?              ]
          [rvs.example.com]                    +-----+
      +------------------------------------------->|     |
      |                                            | DNS |
      | +---------------------------------------|     |
      | |   [HIP?                           ]        +-----+
      | |   [www.example.com                ]
      | |   [HIP HIT-R HI-R rvs.example.com]
      | |
      | |   [A?              ]
      | |   [rvs.example.com]
      | |   [A IP-RVS        ]
      | |
      | |                +-----+
      | | +------I1----->| RVS |-----I1------+
      | | |              +-----+             |
      | | |                                  |
      | | |                                  |
      | v |                                  v
    +-----+                          +-----+
    |     |<---------------R1------------|     |
    |  I  |---------------I2----------->|  R  |
    |     |<---------------R2------------|     |
    +-----+                          +-----+
```

The initiator would then send an I1 to the RVS IP address (IP-RVS.)
Following, the RVS will relay the I1 up to the mobile node's IP
address (IP-R), which will complete the HIP exchange.

4. Overview of using the DNS with HIP

4.1. Storing HI, HIT and RVS in DNS

   Any conforming implementation may store a Host Identity (HI) and its
   associated Host Identity Tag (HIT) in a DNS HIP RDATA format. If a
   particular form of an HI does not already have a specified RDATA
   format, a new RDATA-like format SHOULD be defined for the HI. HI and
   HIT are defined in Section 3 of [I-D.ietf-hip-base].

   Upon return of a HIP RR, a host MUST always calculate the HI-
   derivative HIT to be used in the HIP exchange, as specified in
   Section 3 of the HIP base specification [I-D.ietf-hip-base], while
   the HIT possibly embedded along SHOULD only be used as an
   optimization (e.g. table lookup.)

   The HIP resource record may also contain one or more domain name(s)
   of rendezvous server(s) towards which HIP I1 packets might be sent to
   trigger the establishment of an association with the entity named by
   this resource record [I-D.ietf-hip-rvs].

   The rendezvous server field of the HIP resource record stored at a
   given domain name MAY include the domain name itself. A semantically
   equivalent situation occurs if no rendezvous server is stored in the
   HIP resource record of that domain. Such situations occurs in two
   cases:

   o The host is mobile, and the A and/or AAAA resource record(s)
      stored at its domain name contains the IP address(es) of its
      rendezvous server rather than its own one.

   o The host is stationary, and can be reached directly at IP
      address(es) contained in A and/or AAAA resource record(s) stored
      at its domain name. This a degenerated case of rendezvous service
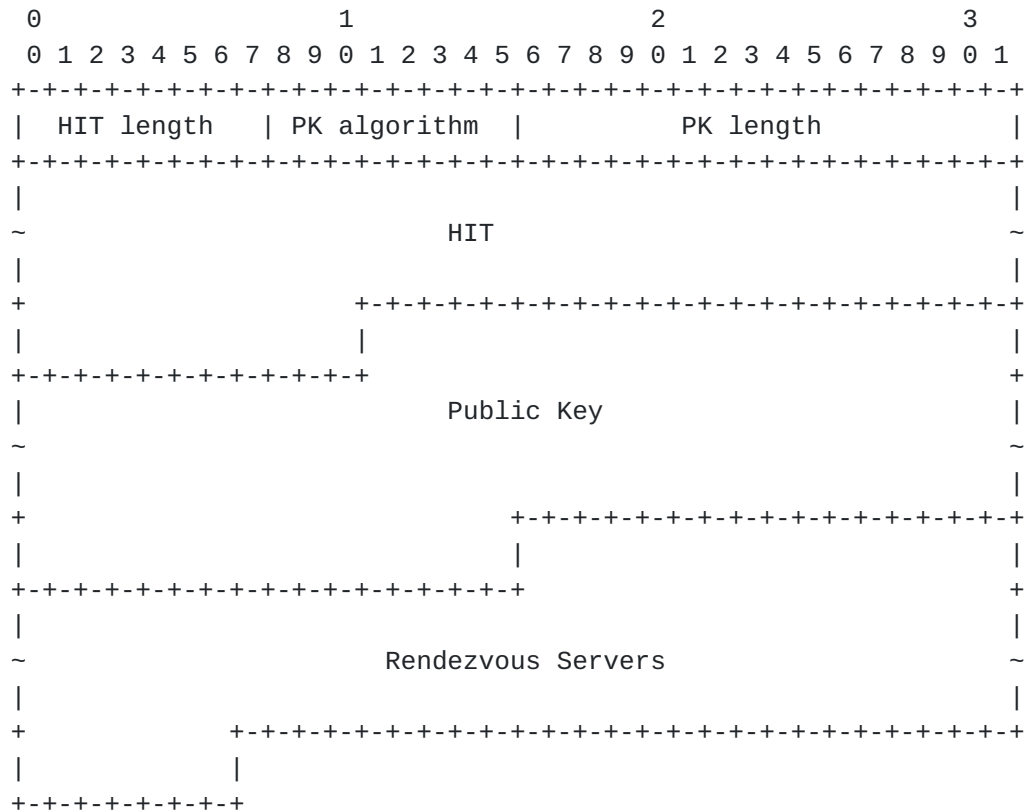   where the host somewhat acts as a rendezvous server for itself.

   An RVS receiving such an I1 would then relay it to the appropriate
   responder (the owner of the I1 receiver HIT.) The responder will
   then complete the exchange with the initiator, typically without
   ongoing help from the RVS.

4.2. Initiating connections based on DNS names

   On a HIP node, a Host Identity Protocol exchange SHOULD be initiated
   whenever an Upper Layer Protocol attempts to communicate with an
   entity and the DNS lookup returns HIP resource records.

5. HIP RR Storage Format

   The RDATA for a HIP RR consists of a public key algorithm type, the
   HIT length, a HIT, a public key, and optionally one or more
   rendezvous server(s).

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  HIT length   | PK algorithm  |          PK length            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                            HIT                                ~
|                                                               |
+                     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     |                                         |
+-+-+-+-+-+-+-+-+-+-+-+                                         +
|                          Public Key                          |
~                                                              ~
|                                                               |
+                     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     |                                         |
+-+-+-+-+-+-+-+-+-+-+-+-+                                       +
|                                                               |
~                      Rendezvous Servers                       ~
|                                                               |
+            +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            |
+-+-+-+-+-+-+-+
```

   The HIT length, PK algorithm, PK length, HIT and Public Key field are
   REQUIRED. The Rendezvous Servers field is OPTIONAL.

5.1. HIT length format

   The HIT length indicates the length in bytes of the HIT field. This
   is an 8 bits unsigned integer.

5.2. PK algorithm format

   The PK algorithm field indicates the public key cryptographic
   algorithm and the implied public key field format. This is an 8 bits
   unsigned integer. This document reuses the values defined for the
   'algorithm type' of the IPSECKEY RR [RFC4025] 'gateway type' field.

   The presently defined values are shown here for reference:

1 A DSA key is present, in the format defined in RFC2536
[RFC2536].

2 A RSA key is present, in the format defined in RFC3110
[RFC3110].

5.3. PK length format

The PK length indicates the length in bytes of the Public key field.
This is a 16 bits unsigned integer in network byte order.

5.4. HIT format

The HIT is stored, as a binary value, in network byte order.

5.5. Public key format

Both of the public key types defined in this document (RSA and DSA)
reuse the public key formats defined for the IPSECKEY RR [RFC4025]
(which in turns contains the algorithm-specific portion of the KEY RR
RDATA, all of the KEY RR DATA after the first four octets,
corresponding to the same portion of the KEY RR that must be
specified by documents that define a DNSSEC algorithm.)

In the future, if a new algorithm is to be used both by IPSECKEY RR
and HIP RR, it should use the same public key encoding for both RRs.
Unless specified otherwise, the HIP RR public key field SHOULD use
the same public key format as the IPSECKEY RR RDATA for the
corresponding algorithm.

The DSA key format is defined in RFC2536 [RFC2536].

The RSA key format is defined in RFC3110 [RFC3110] and the RSA key
size limit (4096 bits) is relaxed in the IPSECKEY RR [RFC4025]
specification.

5.6. Rendezvous servers format

The Rendezvous servers field indicates one or more variable length
wire-encoded domain names rendezvous server(s), as described in
Section 3.3 of RFC1035 [RFC1035]. The wire-encoded format is self-
describing, so the length is implicit. The domain names MUST NOT be
compressed. The rendezvous server(s) are listed in order of
preference (i.e. first rendezvous server(s) are preferred).

[6](#). **HIP RR Presentation Format**

   This section specifies the representation of the HIP RR in a zone
   data master file.

   The HIT length field is not represented as it is implicitly known
   thanks to the HIT field representation.

   The PK algorithm field is represented as unsigned integers.

   The PK length field is not represented as it is implicitly known
   thanks to the Public key field representation.

   The HIT field is represented as the Base16 encoding [RFC3548] (a.k.a.
   hex or hexadecimal) of the HIT. The encoding MUST NOT contain
   whitespace(s).

   The Public Key field is represented as the Base64 encoding [RFC3548]
   of the public key. The encoding MAY contain whitespace(s), and such
   whitespace(s) MUST be ignored.

   The Rendezvous servers field is represented by one or more
   uncompressed domain name(s)

   The complete representation of the HPIHI record is:

   IN HIP   (pk-algorithm
               base16-encoded-hit
               base64-encoded-public-key
               rendezvous-server[1]
                      ...
               rendezvous-server[n])

7. Examples

   Example of a node with HI and HIT but no RVS:

```
www.example.com.       IN  HIP ( 2 4009D9BA7B1A74DF365639CC39F1D578
                             AwEAAbdxyhNuSutc5EMzxTs9LBPCIkOFH8cIv
                             M4p9+LrV4e19WzK00+CI6zBCQTdtWsuxKbWIy
                             87UOoJTwkUs7lBu+Upr1gsNrut79ryra+bSRG
                             Qb1slImA8YVJyuIDsj7kwzG7jnERNqnWxZ48A
                             WkskmdHaVDP4BcelrTI3rMXdXF5D )
```

   Example of a node with a HI, HIT and one RVS:

```
www.example.com.       IN  HIP ( 2 4009D9BA7B1A74DF365639CC39F1D578
                             AwEAAbdxyhNuSutc5EMzxTs9LBPCIkOFH8cIv
                             M4p9+LrV4e19WzK00+CI6zBCQTdtWsuxKbWIy
                             87UOoJTwkUs7lBu+Upr1gsNrut79ryra+bSRG
                             Qb1slImA8YVJyuIDsj7kwzG7jnERNqnWxZ48A
                             WkskmdHaVDP4BcelrTI3rMXdXF5D
                             rvs.example.com )
```


   Example of a node with a HI, HIT and two RVS:

```
www.example.com.       IN  HIP ( 2 4009D9BA7B1A74DF365639CC39F1D578
                             AwEAAbdxyhNuSutc5EMzxTs9LBPCIkOFH8cIv
                             M4p9+LrV4e19WzK00+CI6zBCQTdtWsuxKbWIy
                             87UOoJTwkUs7lBu+Upr1gsNrut79ryra+bSRG
                             Qb1slImA8YVJyuIDsj7kwzG7jnERNqnWxZ48A
                             WkskmdHaVDP4BcelrTI3rMXdXF5D
                             rvs1.example.com
                             rvs2.example.com )
```

8. Security Considerations

   Though the security considerations of the HIP DNS extensions still
   need to be more investigated and documented, this section contains a
   description of the known threats involved with the usage of the HIP
   DNS extensions.

   In a manner similar to the IPSECKEY RR [RFC4025], the HIP DNS
   Extensions allows to provision two HIP nodes with the public keying
   material (HI) of their peer. These HIs will be subsequently used in
   a key exchange between the peers. Hence, the HIP DNS Extensions
   introduce the same kind of threats that IPSECKEY does, plus threats
   caused by the possibility given to a HIP node to initiate or accept a
   HIP exchange using "opportunistic" or "unpublished initiator HI"
   modes.

   A HIP node SHOULD obtain HIP RRs from a trusted party trough a secure
   channel insuring proper data integrity of the RRs. DNSSEC [RFC2065]
   provides such a secure channel.

   In the absence of a proper secure channel, both parties are
   vulnerable to MitM and DoS attacks, and unrelated parties might be
   subject to DoS attacks as well. These threats are described in the
   following sections.

8.1. Attacker tampering with an insecure HIP RR

   The HIP RR contains public keying material in the form of the named
   peer's public key (the HI) and its secure hash (the HIT.) Both of
   these are not sensitive to attacks where an adversary gains knowledge
   of them. However, an attacker that is able to mount an active attack
   on the DNS, i.e., tampers with this HIP RR (e.g. using DNS spoofing)
   is able to mount Man-in-the-Middle attacks on the cryptographic core
   of the eventual HIP exchange (responder's HIP RR rewritten by the
   attacker.)

   The HIP RR may contain a rendezvous server domain name resolved into
   a destination IP address where the named peer is reachable by an I1
   (HIP Rendezvous Extensions IPSECKEY RR [I-D.ietf-hip-rvs].) Thus, an
   attacker able to tamper with this RR is able to redirect I1 packets
   sent to the named peer to a chosen IP address, for DoS or MitM
   attacks. Note that this kind of attack is not specific to HIP and
   exists independently to whether or not HIP and the HIP RR are used.
   Such an attacker might tamper with A and AAAA RRs as well.

   An attacker might obviously use these two attacks in conjunction: It
   will replace the responder's HI and RVS IP address by its owns in a
   spoofed DNS packet sent to the initiator HI, then redirect all

exchanged packets to him and mount a MitM on HIP. In this case HIP
won't provide confidentiality nor initiator HI protection from
eavesdroppers.

8.2. Hash and HITs Collisions

As many cryptographic algorithm, some secure hashes (e.g. SHA1, used
by HIP to generate a HIT from an HI) eventually become insecure,
because an exploit has been found in which an attacker with a
reasonable computation power breaks one of the security features of
the hash (e.g. its supposed collision resistance.) This is why a HIP
end-node implementation SHOULD NOT authenticate its HIP peers based
solely on a HIT retrieved from DNS, but SHOULD rather use HI-based
authentication.

8.3. DNSSEC

In the absence of DNSSEC, the HIP RR is subject to the threats
described in RFC 3833 [RFC3833].

9. IANA Considerations

    IANA should allocate one new RR type code (TBD, 55?) for the HIP RR
    from the standard RR type space.

    IANA does not need to open a new registry for public key algorithms
    of the HIP RR because the HIP RR reuses "algorithms types" defined
    for the IPSECKEY RR [RFC4025]. The presently defined values are
    shown here for reference:

        0 is reserved

        1 is RSA

        2 is DSA

10. Acknowledgments

   As usual in the IETF, this document is the result of a collaboration
   between many people. The authors would like to thanks the author
   (Michael Richardson), contributors and reviewers of the IPSECKEY RR
   [RFC4025] specification, which this document was framed after. The
   authors would also like to thanks the following people, who have
   provided thoughtful and helpful discussions and/or suggestions, that
   have helped improving this document: Jeff Ahrenholz, Rob Austein,
   Hannu Flinck, Tom Henderson, Olaf Kolkman, Miika Komu, Andrew
   McGregor, Erik Nordmark, and Gabriel Montenegro. Some parts of this
   draft stem from [I-D.ietf-hip-base].

   Julien Laganier is partly funded by Ambient Networks, a research
   project supported by the European Commission under its Sixth
   Framework Program. The views and conclusions contained herein are
   those of the authors and should not be interpreted as necessarily
   representing the official policies or endorsements, either expressed
   or implied, of the Ambient Networks project or the European
   Commission.

11. References

11.1. Normative references

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities",
           STD 13, RFC 1034, November 1987.

[RFC1035] Mockapetris, P., "Domain names - implementation and
           specification", STD 13, RFC 1035, November 1987.

[RFC2065] Eastlake, D. and C. Kaufman, "Domain Name System Security
           Extensions", RFC 2065, January 1997.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
           Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2536] Eastlake, D., "DSA KEYs and SIGs in the Domain Name System
           (DNS)", RFC 2536, March 1999.

[RFC3110] Eastlake, D., "RSA/SHA-1 SIGs and RSA KEYs in the Domain
           Name System (DNS)", RFC 3110, May 2001.

[RFC3363] Bush, R., Durand, A., Fink, B., Gudmundsson, O., and T.
           Hain, "Representing Internet Protocol version 6 (IPv6)
           Addresses in the Domain Name System (DNS)", RFC 3363,
           August 2002.

[RFC3548] Josefsson, S., "The Base16, Base32, and Base64 Data
           Encodings", RFC 3548, July 2003.

[RFC3596] Thomson, S., Huitema, C., Ksinant, V., and M. Souissi,
           "DNS Extensions to Support IP Version 6", RFC 3596,
           October 2003.

[RFC4025] Richardson, M., "A Method for Storing IPsec Keying
           Material in DNS", RFC 4025, March 2005.

[I-D.ietf-hip-base]
           Moskowitz, R., "Host Identity Protocol",
           draft-ietf-hip-base-06 (work in progress), June 2006.

[I-D.ietf-hip-rvs]
           Laganier, J. and L. Eggert, "Host Identity Protocol (HIP)
           Rendezvous Extension", draft-ietf-hip-rvs-05 (work in
           progress), June 2006.

11.2. Informative references

[I-D.ietf-hip-arch]
          Moskowitz, R. and P. Nikander, "Host Identity Protocol
          Architecture", draft-ietf-hip-arch-03 (work in progress),
          August 2005.

[I-D.ietf-hip-mm]
          Nikander, P., "End-Host Mobility and Multihoming with the
          Host Identity Protocol", draft-ietf-hip-mm-04 (work in
          progress), June 2006.

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an
          IANA Considerations Section in RFCs", BCP 26, RFC 2434,
          October 1998.

[RFC3833] Atkins, D. and R. Austein, "Threat Analysis of the Domain
          Name System (DNS)", RFC 3833, August 2004.

Authors' Addresses

    Pekka Nikander
    Ericsson Research Nomadic Lab
    JORVAS FIN-02420
    FINLAND

    Phone: +358 9 299 1
    Email: pekka.nikander@nomadiclab.com

    Julien Laganier
    DoCoMo Communications Laboratories Europe GmbH
    Landsberger Strasse 312
    Munich 80687
    Germany

    Phone: +49 89 56824 231
    Email: julien.ietf@laposte.net
    URI: http://www.docomolab-euro.com/

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment